AC 29.917A. § 29.917 (Amendment 29-40) DESIGN.

a. Explanation. Amendment 29-40 introduces a new § 29.917(b). The previous § 29.917(b) has been redesignated as § 29.917(c). Section 29.917(a) sets forth a definition of the rotor drive system and its associated components and § 29.917(b) requires a design assessment to be performed. The intent of this paragraph (b) is to identify the critical components and to establish and/or clarify their design integrity to show that the basic airworthiness requirements, which are applicable to the rotor drive system, will be met.

b. Procedures.

(1) Section 29.917(a) General. The method of compliance for this section is unchanged.

(2) Section 29.917(b) Design Assessment. A design assessment of the rotor drive system should be carried out in order to substantiate that the system is of a safe design and that compensating provisions are made available to prevent failures classified as hazardous and catastrophic in the sense specified in paragraph (c) below. In carrying out the design assessment, the results of the certification ground and flight testing (including any failures or degradation) should be taken into consideration. Previous service experience with similar designs should also be taken into account (see also § 29.601(a)).

c. Definitions. For the purposes of this assessment, failure conditions may be classified according to the severity of their effects as follows:

(1) Minor. Failure conditions which would not significantly reduce rotorcraft safety, and which involve crew actions that are well within their capabilities. Minor failure conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some inconvenience to occupants.

(2) Major. Failure conditions which would reduce the capability of the rotorcraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to occupants, possibly including injuries.

(3) Hazardous. Failure conditions which would reduce the capability of the rotorcraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be--

(i) A large reduction in safety margins or functional capabilities;

(ii) Physical distress or higher workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely;

(iii) Serious or fatal injury to a relatively small number of the occupants;

(iv) Loss of ability to continue safe flight to a suitable landing site.

(4) Catastrophic. Failure conditions which would prevent a safe landing.

(5) Minimize. Reduce to the least possible amount by means that can be shown to be both technically feasible and economically justifiable.

(6) Health Monitoring. Equipment, techniques, and/or procedures by which selected incipient failure or degradation can be determined.

d. Failure Analysis.

(1) The first stage of the design assessment should be the Failure Analysis, by which all the hazardous and catastrophic failure modes are identified. The failure analysis may consist of a structured, inductive bottom-up analysis, which is used to evaluate the effects of failures on the system and on the aircraft for each possible item or component failure. When properly formatted it will aid in identifying latent failures and the possible causes of each failure mode. The failure analysis should take into consideration all reasonably conceivable failure modes in accordance with the following:

(i) Each item/component function(s).

(ii) Item/component failure modes and their causes.

(iii) The most critical operational phase/mode associated with the failure mode.

(iv) The effects of the failure mode on the item/component under analysis, the secondary effects on the rotor drive system and on the rotors, on other systems and on the rotorcraft. Combined effects of failures should be analyzed where a primary failure is likely to result in a secondary failure.

(v) The safety device or health monitoring means by which occurring or incipient failure modes are detected, or their effects mitigated. The analysis should consider the safety system failure.

(vi) The compensating provision(s) made available to circumvent or mitigate the effect of the failure mode (see also paragraph (1) below).

(vii) The failure condition severity classification according to the definitions given in paragraph (c) above.

(2) When deemed necessary for particular system failures of interest, the above analysis may be supplemented by a structured, deductive top-down analysis, which is used to determine which failure modes contribute to the system failure of interest.

(3) Dormant failure modes should be analyzed in conjunction with at least one other failure mode for the specific component or an interfacing component. This latter failure mode should be selected to represent a failure combination with potential worst-case consequences.

(4) When significant doubt exists as to the effects of a failure, these effects may be required to be verified by tests.

e. Evaluation of Hazardous and Catastrophic Failures.

(1) The second stage of the design assessment is to summarize the hazardous and catastrophic failures and appropriately substantiate the compensating provisions that are made available to minimize the likelihood of their occurrence. Those failure conditions that are more severe should have a lower likelihood of occurrence associated with them than those that are less severe. The applicant should obtain early concurrence of the cognizant certificating authority with the compensating provisions for each hazardous or catastrophic failure.

(2) Compensating provisions may be selected from one or more of those listed below, but not necessarily limited to this list.

(i) Design features; i.e., safety factors, part-derating criteria, redundancies, etc.

(ii) A high level of integrity: All parts with catastrophic failure modes and critical characteristics are to be identified as Critical Parts and be subject to a Critical Parts Plan (see AC 29.602.). Where a high level of integrity is used as a compensating provision, parts with a hazardous failure mode which would prevent continued safe flight may be included in a Critical Parts Plan or subjected to other enhancements to the normal control procedures for parts.

(iii) Fatigue tolerance evaluation.

(iv) Flight limitations.

(v) Emergency procedures.

(vi) An inspection or check that would detect the failure mode or evidence of conditions that could cause the failure mode.

(vii) A preventive maintenance action to minimize the likelihood of occurrence of the failure mode, including replacement actions and verification of serviceability of items which may be subject to a dormant failure mode.

(viii) Special assembly procedures or functional tests for the avoidance of assembly errors which could be safety critical.

(ix) Safety devices or health monitoring means beyond those identified in paragraphs (vi) and (vii) above.